REMARKS/ARGUMENTS

In the Office action dated March 21, 2001 the Examiner rejected claims 1 - 22 under 35 U.S.C. § 103. Applicant hereby amends the application and requests reconsideration and reexamination of the claims. Applicant has canceled claims 5, 6, 10, 11 and 13 and added claims 23 - 27. Applicant also has amended the specification to correct a typographical error. Claims 1 - 4, 7 - 9, 12 and 14 - 27 are now pending in this application.

Response to the Rejection of the Claims Under 35 U.S.C. § 103

The Examiner rejected claims 1 - 6 and 9 - 22 under 35 U.S.C. § 103(a) as being unpatentable over Hobson et al., U.S. Patent No. 6,209,016 (hereafter referred to as "Hobson") in view of Fischer et al., U.S. Patent No. 6,237,016) hereafter referred to as "Fischer"). The Examiner rejected claims 7 and 8 under 35 U.S.C. § 103(a) as being unpatentable over Hobson in view of Fischer as applied to claim 1 and further in view of Curiger et al., U.S. Patent No. 6,064,740. Claims 1, 21 and 22 are independent. Claims 2 - 4, 7 - 9, 12, 14 - 20 and 23 - 27 depend on independent claim 1.

Independent claims 1, 21 and 22 are not obvious in view of the cited references because there was no motivation to combine these references in a manner that provides the claimed inventions and, even assuming there was motivation to combine these references, the combination does not teach or suggest the invention of claim 1, 21 or 22.

The combination of Hobson and Fischer is improper in this case because at the time the invention was made there was no motivation in the art to combine the two references. Hobson is directed to a co-processor for performing modular multiplication. Hobson, Abstract. In contrast, Fischer is directed to a method and apparatus for performing complex digital filters. Fischer, Abstract.

The Hobson disclosure is totally unrelated to the subject matter of Fischer, namely filter design. Hobson does not even contain a single reference to a filter. Moreover, there is no evidence of any suggestion that the techniques used in modular multiplication would be useful in filter design. Accordingly one skilled in the art looking to improve Fischer would not have looked to Hobson for improvements.

Conversely, the Fischer disclosure is totally unrelated to the subject matter of Hobson, namely modular operations. Fischer does not contain a single reference to modular operations. There also is no evidence of any suggestion that the techniques used in filter design would be useful in modular operations. Accordingly, one skilled in the art looking to improve Hobson would not have looked to Fischer for assistance.

In view of the above, there would not have been any motivation to one skilled in the art to combine Hobson and Fischer. Accordingly, the obviousness rejection based on this combination should be withdrawn.

Moreover, the combination of Hobson and Fischer does not provide the invention of claim 1, 21 or 22. For example, neither Hobson nor Fischer teach or suggest performing

"specified multiplication and addition operations in parallel" as claimed in claim 1 or performing "simultaneous multiplication and addition operations" as claimed in claims 21 and 22.

Hobson discloses at column 4, lines 22 - 67, in part:

> The new co-processor uses bit-pair multiplication, addition and subtraction. Instead of using a single serial loop clocking scheme as in the co-processor of FIG. 1, the serial bit stream in the new improved co-processor is examined two bits at a time per clock period.
>
> As will be described in detail below, each serial bit stream is split into two (odd and even) component bit streams (bits from the originating serial bit stream being fed alternately into the two component serial bit streams respectively) and the two component bit streams are processed in parallel, one bit being presented by each of the component bit streams at the same time to form a bit-pair for calculation. This means that the adders, subtracters and parallel-serial multipliers evaluate and compute results two bits at a time.

Hobson thus discloses in Figure 2 an improvement of the circuit of Figure 1 where the bit stream is divided in two and provided to two parallel circuits. Each circuit, however, performs each distinct operation serially. Thus, Hobson merely teaches that the multiplication operation for each stream may be performed in parallel at a given point during the serial process or addition operations for each stream performed in parallel at a given point during the serial process. Hobson does not teach,

however, that addition and multiplication operations are performed in parallel or simultaneously.

The parallel operations of Fischer are described in conjunction with Figures 2A and 2B. Figure 2B illustrates that the multiply operations are performed in parallel (multipliers 260 - 266). In addition, Figure 2B illustrates that the addition operations are performed in parallel (adders 270 - 272). Figure 2B also illustrates, however, that the addition operations are performed after the multiplication operations. Thus the multiplication and addition operations are not performed in parallel or simultaneously.

Moreover, neither of the references teaches or suggests that one of two different types of parallel operations may be selected based on an instruction. For example, the circuit of Hobson always performs the same parallel operations. Hobson does not configure the circuit at one time to perform multiplication operations in parallel based on an instruction, then configure the circuit at another time to perform multiplication and addition operations in parallel based on an instruction.

Similarly, Fischer does not reconfigure the parallel operations that it performs to provide either parallel multiplication operations or parallel multiplication and addition operations based on an instruction. Rather Fischer switches between multiply-add and multiply subtract operations.

Distinguishing features of the invention are clearly set forth in the claims. For example, claim 1 recites, in part:

an execution unit configured to execute product and square operations, the execution unit including at least one adder and at least two multipliers configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel;

a decode unit, coupled to the execution unit, the decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, the decode unit further configured to issue instructions so that the execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either the square or product operation.

Claim 21 recites, in part:

issuing, by the decode unit, a first instruction to perform a Montgomery square operation;

issuing, by the decode unit, a second instruction to perform a Montgomery product operation;

performing, by an execution unit, simultaneous multiplication operations in response to at least one of the first instruction and the second instruction; and

performing, by the execution unit, simultaneous multiplication and addition operations in response to at least one of the first instruction and the second instruction.

Claim 21 recites, in part:

issuing, by the decode unit, a first set of instructions for an execution unit to perform the Montgomery square operation, the first set of instructions comprising:

a first instruction to perform simultaneous multiplication operations; and

a second instruction to perform simultaneous multiplication and addition operations; and

issuing, by the decode unit, a second set of instructions for an execution unit to perform the Montgomery product operation, the second set of instructions comprising:

a third instruction to perform simultaneous multiplication operations;

a fourth instruction to perform simultaneous multiplication and addition operations; and

a fifth instruction to perform simultaneous multiplication and addition operations.

In view of the above Applicant submits that the cited references do not teach or suggest the invention of claim 1, 21 or 22.

Claims 2 - 4, 7 - 9, 12, 14 - 20 and 23 - 27 that depend on claim 1 also are patentable over the cited references for the reasons set forth above. In addition, these dependent claims are patentable over these references for the additional limitations that the dependent claims contain.

CONCLUSION

In view of the above amendment and remarks it is submitted that the claims are patentably distinct over the cited references and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
SDB PAS617010.1-*-06/21/05 11:41 PM